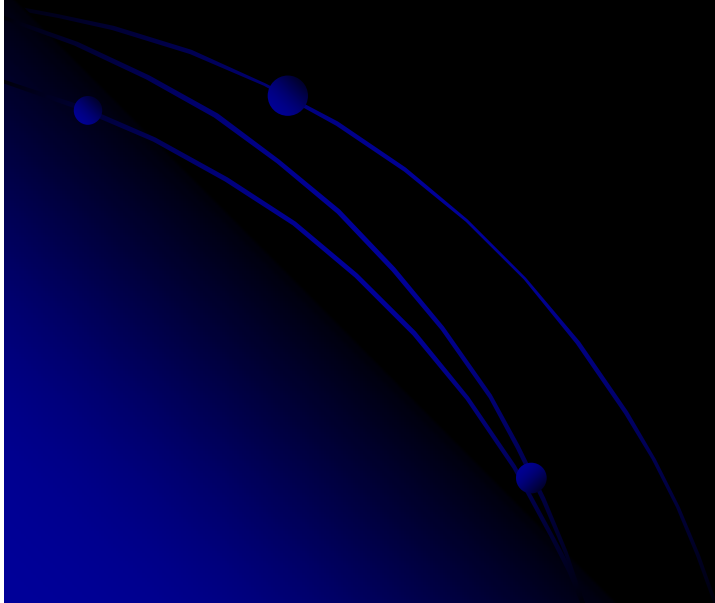


Division of Workforce Development

Confidentiality and Information Security Plan



DEFINITIONS:

Disclosure:

To disclose, release, transfer, disseminate or otherwise communicate all or any part of confidential information/records/data verbally, in writing, electronically or by any other means to any person or entity.

DEFINITIONS:

Authorized Users:

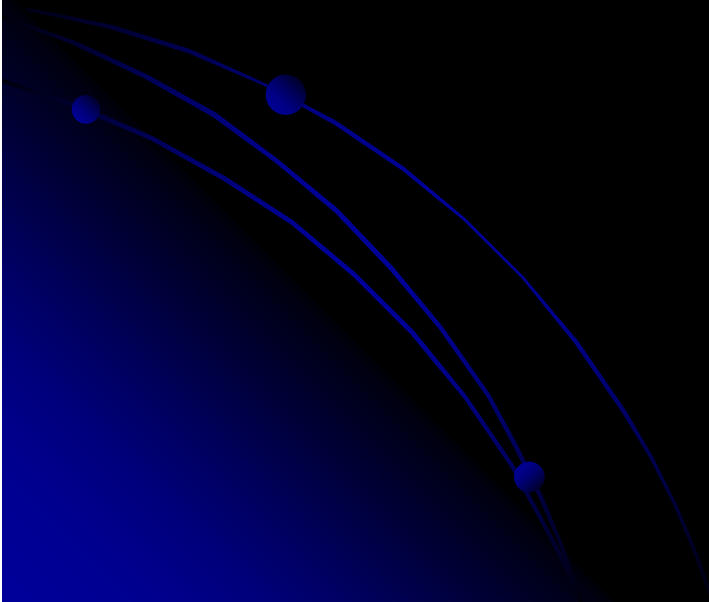
- Workforce investment system staff
- Consultants
- Other subcontracting entities
- Any other person having routine access to workforce investment system confidential information/data

These users must be identified on the appropriate entity's Authorized User List.

DEFINITIONS:

Confidential Information:

Any **information** that **identifies** or **describes** an **individual** or **employer**.



DEFINITIONS:

Confidential Information:

Includes, but not limited to:

- name
- social security number
- ethnicity
- age
- date of birth
- gender

DEFINITIONS:

Confidential Information:

Includes, but not limited to:

- home address
- telephone number
- physical description
- family and household composition
- domestic violence
- education
- medical history

DEFINITIONS:

Confidential Information:

Includes, but not limited to:

- employment history
- wages
- Federal employer identification number (FEIN)
- North American Industrial Classification System (NAICS) and industry codes

DEFINITIONS:

Confidential Information:

Includes, but not limited to:

- unemployment insurance payments or status
- account information
- financial matters

Confidential information also includes **statements** made by, or attributed to, the individual or employer.

DEFINITIONS:

Partners or Partner Agencies:

Any agency that is part of the Career Center system, besides DWD. These include:

- Department of Labor and Industrial Relations (DOLIR)
- Family Support Division (FSD)
- Department of Corrections (DOC)
- Department of Elementary and Secondary Education (DESE)...

DEFINITIONS:

Partners or Partner Agencies (cont.):

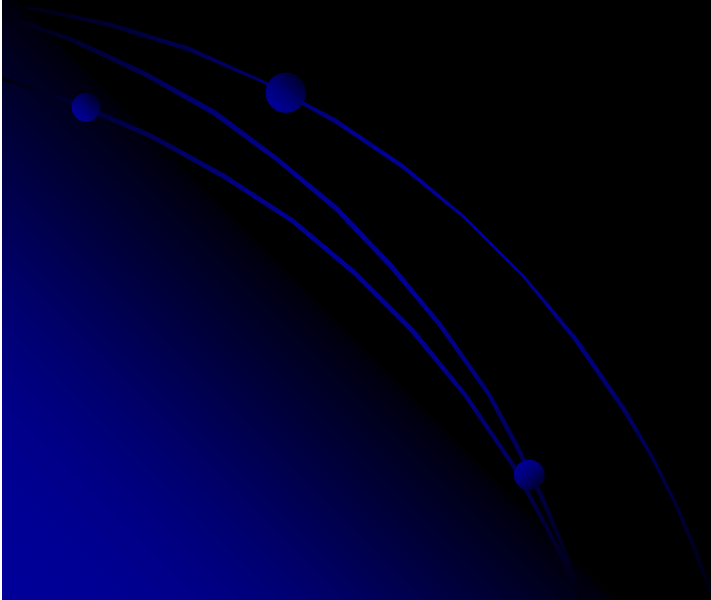
- Information Technology Support Division (ITSD)
- Department of Health and Senior Services (DHSS)
- Local Workforce Investment Boards (WIBs)
- Their contractor agencies

INTRODUCTION

The public workforce investment system consists of the **Division of Workforce Development (DWD)**, local workforce investment boards **(WIBs)** and their contractors and sub-contractors, as well as partner agencies.

INTRODUCTION

All of these entities use various forms of confidential information in their day-to-day operations.

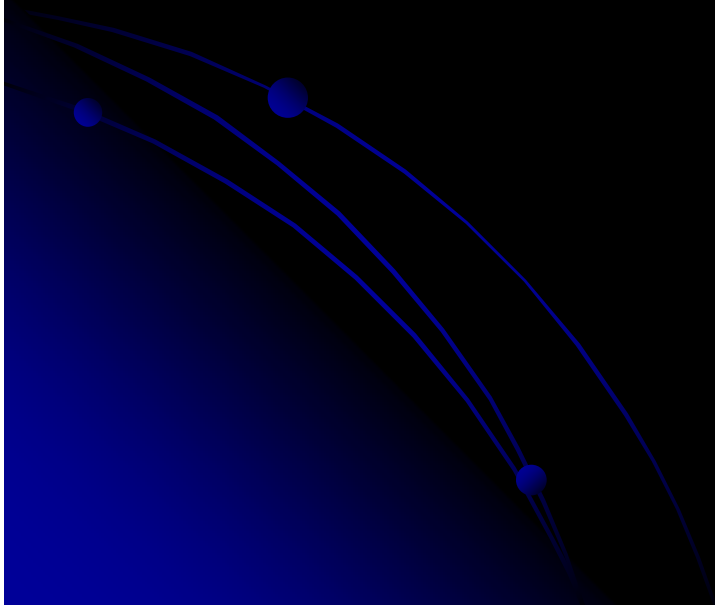


INTRODUCTION

The purpose of this plan is to identify sources of confidential information and establish procedures for the safe handling of this information so it is not accessed by unauthorized individuals.

INTRODUCTION

Maintaining confidential records is important for obvious reasons to the individual, including the prevention of identity theft.



INTRODUCTION

- Any WIB that has a confidentiality plan should ensure that their plan is in concurrence with this plan.
- WIBs are responsible for ensuring that their contractors' confidentiality policies are in concurrence with this policy.

SOURCES OF CONFIDENTIAL INFORMATION

Customer individual record files

(paper copy, Toolbox case files, etc.)

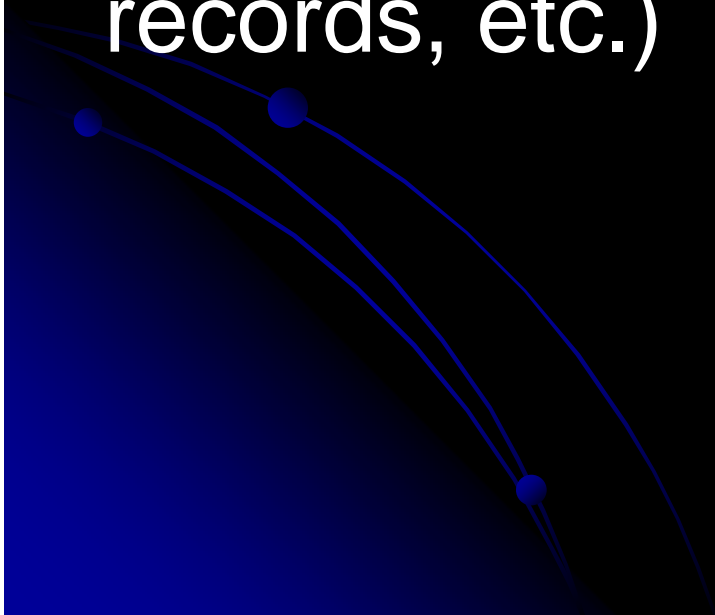
- Includes all eligibility documentation, as required by DWD Issuance 13-99, as amended, Technical Assistance
- Guidance on Documentation / Verification Systems for Title I of WIA.

SOURCES OF CONFIDENTIAL INFORMATION

Customer individual record files

(paper copy, Toolbox case files, etc.)

- Toolbox DWD Reports (Employment and Training Reports, assessment records, etc.)



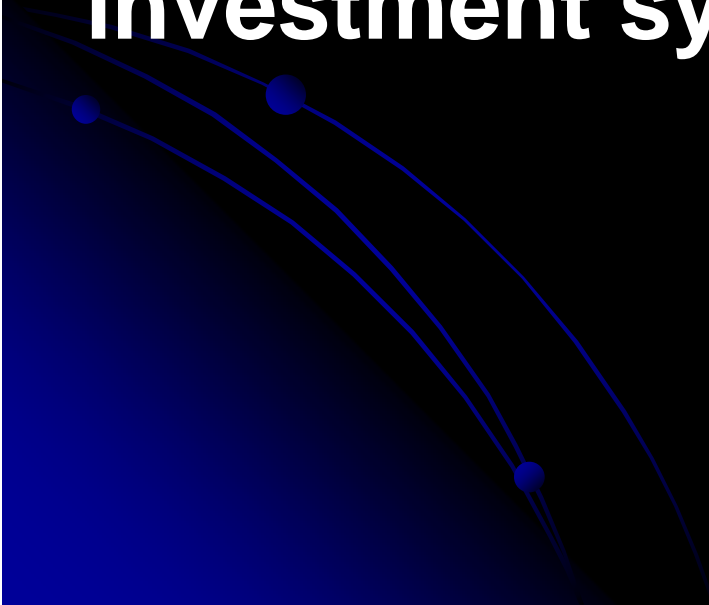
SOURCES OF CONFIDENTIAL INFORMATION (cont.)

- **Mo Performs** (by FutureWork Systems)
- **Unemployment Insurance (UI) wage records**
- **Wage Record Interchange System (WRIS) data**

SOURCES OF CONFIDENTIAL INFORMATION

- **DWD oversees or operates various federal and state programs that collect confidential information on customers.**
- **In addition to these programs,**
- **local workforce investment boards contract with service providers, who also must utilize confidential information in their operations.**

SOURCES OF CONFIDENTIAL INFORMATION

- A customer's confidential information may be shared among various authorized staff of partner agencies that coordinate their services through the workforce investment system.
- 

LEGAL REQUIREMENTS

- Various programs and services offered through the local workforce system are covered by numerous **state and federal legal provisions.**

(See Section 6 for a listing of some of these legal provisions.)

PROCEDURES—Potential Authorized Users

- **DWD Central Office staff** that have access to confidential information include:

- **Director**
- **Assistant Director**
- **Program Administrators**
- **Managers and their staff.**

PROCEDURES—Potential Authorized Users

- Others with access may include staff from:

- **ITSD**
- **PAR**
- **JOBSTAT**
- **Skill Development Center**
- **Federal program staff**
- **Other staff designated by their supervisor**

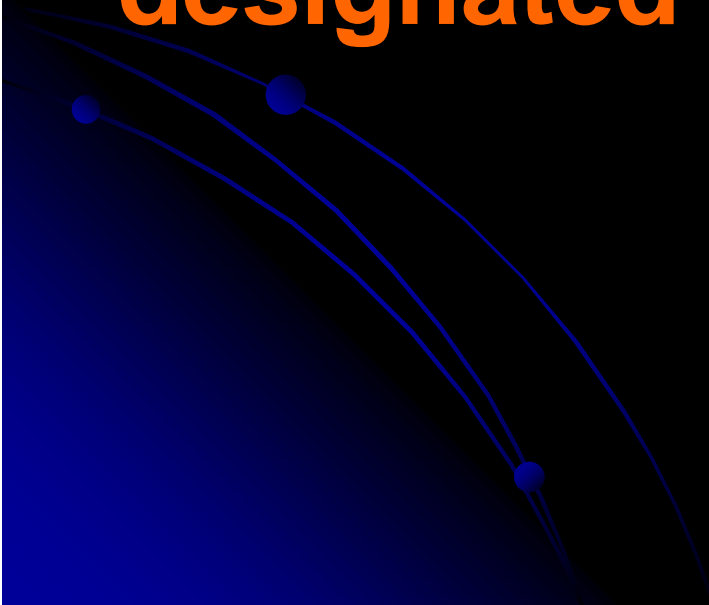
PROCEDURES—Potential Authorized Users

Local staff with access to confidential information includes:

- **Workforce Investment Board members and staff**
- **WIB contractors (20 CFR, Section 667.410 (a) (2))**
- **One-Stop Site Managers (i.e., functional managers)**
- **partner agency staff**
- **local DWD staff**

PROCEDURES—Potential Authorized Users

It is the **responsibility** of the various organizations' **supervisors** to determine which individuals should be designated as authorized users.



PROCEDURES—Training Authorized Users of Confidential Information

- **Authorized users must complete the required training before they will be allowed to access the confidential information.**

- **Training will be delivered by region**
- 

PROCEDURES—Training Authorized Users of Confidential Information

Authorized users are required to:

- **complete designated mandatory training**
- **sign the User Attestation Form**
(see Section 8.1—copy on next two slides)

FORMS—User Attestation Form, Sect. 8.1

I understand that in the course of my employment with the **Missouri Division of Workforce Development, Department of Economic Development**, I will receive or become aware of information that is sensitive or confidential. This information may be written, electronic, or verbal and come from a variety of sources. I understand that I am not to access sensitive or confidential information unless it is necessary in order for me to complete my job responsibilities.

I further understand that the **Missouri Division of Workforce Development** policy on Confidentiality and Information Security applies to information I may inadvertently hear or see that does not directly involve me in an official capacity. I acknowledge that I must protect all sensitive or confidential information.

FORMS—User Attestation Form, Sect. 8.1

I understand that in the performance of my duties I may be requested to provide sensitive or confidential information to others. I agree to hold in confidence and to not disclose any sensitive or confidential information to any person, including employees of state, federal or local governments, except to those who have an official business reason for the information.

Should I have questions regarding the proper handling and disclosure of confidential or sensitive information, I will immediately notify my supervisor for further clarification and direction prior to releasing the information.

FORMS—User Attestation Form, Sect. 8.1, cont.

If I willfully and knowingly disclose such information in any manner to any person or agency not entitled to receive information, I understand that I may be subject to adverse action, including corrective or disciplinary action, or possibly, personal liability.

I acknowledge that I have received the mandatory training, passed the quiz, and have read, understand, and will adhere to the
_____ *Confidentiality and Information Security*

Department / Institution name

Plan and the above requirements.

Signature

Print Name

Date Signed

Original to official employee file (human resources) and copy to the Authorized User Registry

PROCEDURES—Training Authorized Users of Confidential Information

- Training consists of an **on-line PowerPoint tutorial presentation** and **associated test** which will be made available through Alchemy.
- All authorized users **must complete this training before** they can access confidential information.

PROCEDURES—Training Authorized Users of Confidential Information

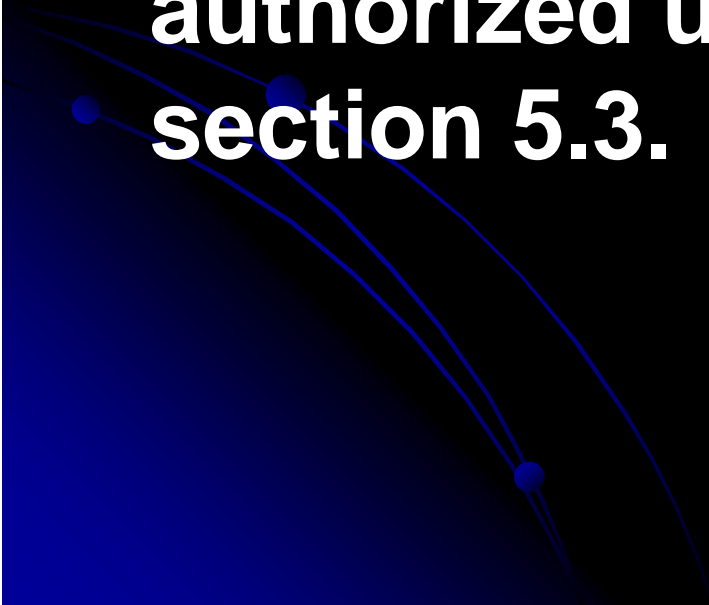
Training is designed to **familiarize all employees with privacy issues and guidelines for the use of confidential data** maintained by DWD, local workforce investment boards and their contractors, and partner agencies.

PROCEDURES—Training Authorized Users of Confidential Information

ALL employees will be required to take training and pass the test prior to requesting access to certain web sites or systems that contain confidential information (such as

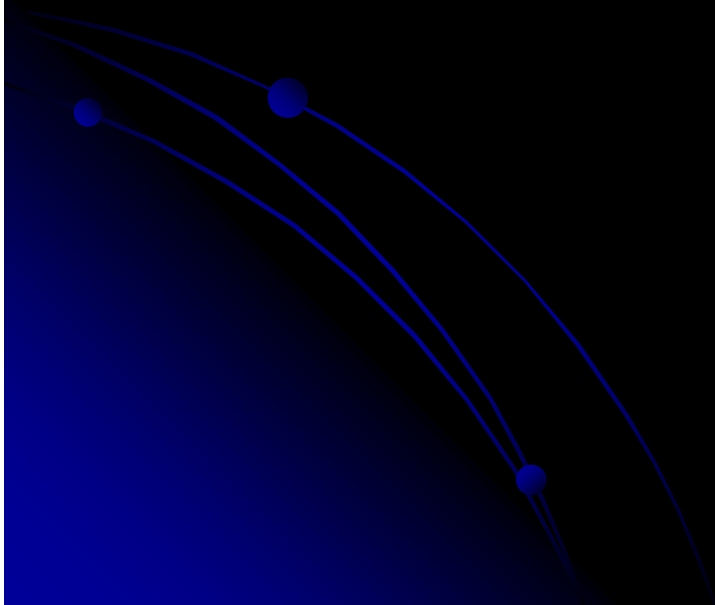
- Toolbox, UI Reporting, MoPerforms, etc.).

PROCEDURES—Training Authorized Users of Confidential Information

- **Toolbox Access Request Forms must be signed by the immediate supervisor and the person responsible for maintaining the authorized user list identified in section 5.3.**
- 

PROCEDURES—Access Eligibility Process

- **DWD Skill Development Center (SDC) will be responsible for maintaining the Authorized User's List of case management system and other on-line data systems.**



PROCEDURES—Access Eligibility Process


- **Local WIB Director and One Stop Site Manager** will **oversee this process for their regions**, including their contractors, to ensure that all partners (except local DWD staff) in their region maintain their authorized user's list appropriately.

PROCEDURES—Access Eligibility Process

- This process should also be addressed in the local **Memorandum of Understanding and/or their local Business Plan.**
- DWD's Quality Assurance may monitor compliance of this as part of the normal monitoring process.

PROCEDURES—Access Eligibility Process

Becoming a new member of the Authorized User's List:

- **view the required PowerPoint**
 - **attain a score of 100% on the Confidentiality Test**
 - **complete the User Attestation Form**
- 

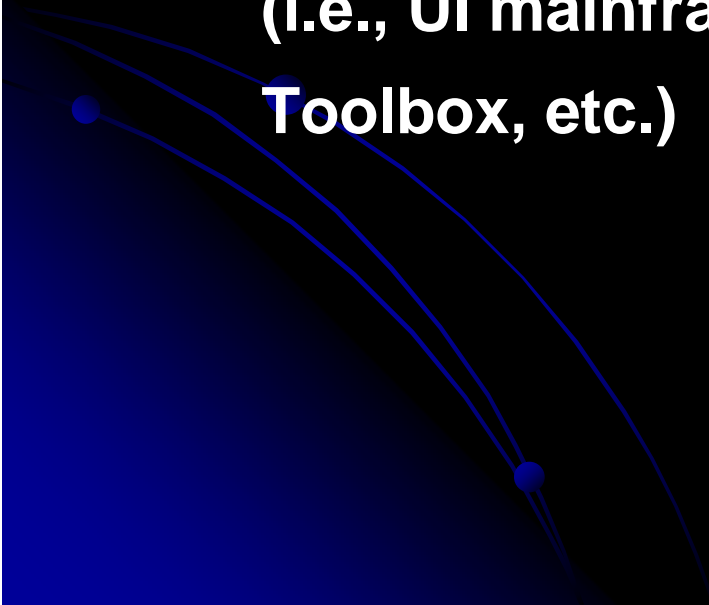
PROCEDURES—Access Eligibility Process

Supervisors of authorized users accessing confidential information:

- responsible for ensuring that these **staff have been trained and submitted User Attestation Form**
- for **DWD employees**, Supervisor **submit their completed User Attestation Form to DED Human Resources** for personnel file
- for **partner agency staff**, Career Center **OSSM submit completed Form to respective agency's personnel contact**

PROCEDURES—Access Eligibility Process

Supervisors of authorized users
accessing confidential information:

- When requesting access for authorized users, the types of information the user will be accessing should also be designated
(i.e., UI mainframe data [Sessions], **MoPerforms**,
Toolbox, etc.)
- 

PROCEDURES—Access Eligibility Process

**DWD's Skill Development Center/
Technical Support Unit will:**

- **provide user access to systems**
- **verify which users may obtain access in systems as appropriate**

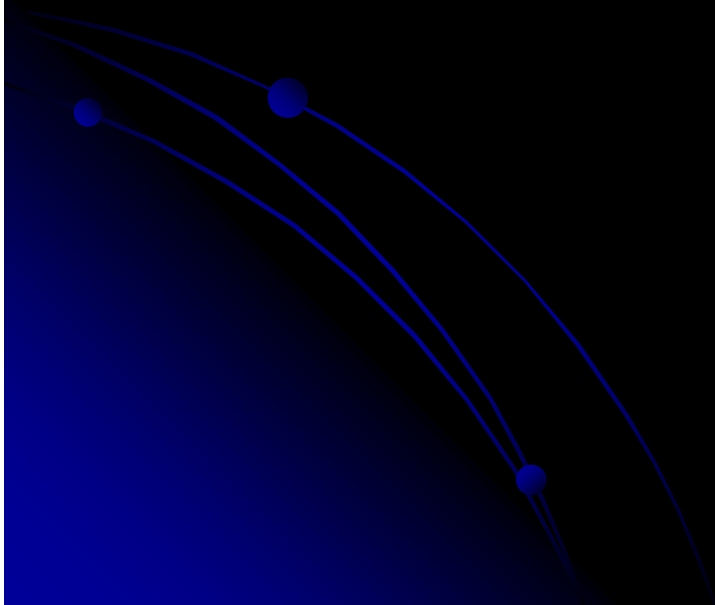
PROCEDURES—Acknowledgement of Confidential Information

Customers:

- **accessing** MissouriCareerSource.com will be made aware that the information they submit is “**only used for the specific purpose for which it is intended. We do not disclose, give, sell or transfer any personal information about our visitors, unless required for law enforcement or statute.**”
- **customers registering with Career Center staff** should be reminded of this statement

PROCEDURES—Acknowledgement of Confidential Information

Paper copies of confidential information should be marked, “Confidential.”



PROCEDURES—Acknowledgement of Confidential Information

Emails and Faxes

- **NOT** considered secure transmissions for confidential information
- Before sending, **verify the accuracy** of email addresses and fax numbers
- When faxing, call recipient to **ensure an authorized user will be receiving fax** upon arrival

PROCEDURES—Acknowledgement of Confidential Information

Emails and Faxes, cont.

- If an **email or fax** with confidential information is **sent or received in error**, **notify the sender/receiver immediately** with instructions for safeguarding the information.

PROCEDURES—Acknowledgement of Confidential Information

Emails and Faxes, cont.

- will **NOT** contain a customer's full social security number
- the **customer's full name**, with **middle initial**, followed by **last five digits of social security number**, or **customer's programmatic identification code** will be used to protect their identity when provided in communication documents

PROCEDURES—Acknowledgement of Confidential Information

Emails and Faxes, cont.

- **Faxes and emails containing confidential information must include the statement on the next slide in the email or on the fax cover sheet.**

NOTE: The fax form available on WorkSmart has been updated to include this language.

PROCEDURES— CONFIDENTIALITY STATEMENT for Emails and Faxes:

The information contained in or attached to this transmission may be confidential and may be protected by legal privilege. It is intended only for the addressee and access to the information in this transmission by anyone other than the addressee is not authorized. Any unauthorized review, copying, distribution, disclosure, or use of this information is strictly prohibited and may be unlawful. If you are not the addressee, please notify the sender immediately and properly destroy this transmission without disclosure.

PROCEDURES—Storage of Confidential Information

- **Any confidential information** in paper copy will be stored in a secure location to prevent access from unauthorized users.
- **Secure locations include:**
 - locked cabinet
 - locked room
 - other means, with access only to authorized users

PROCEDURES—Storage of Confidential Information

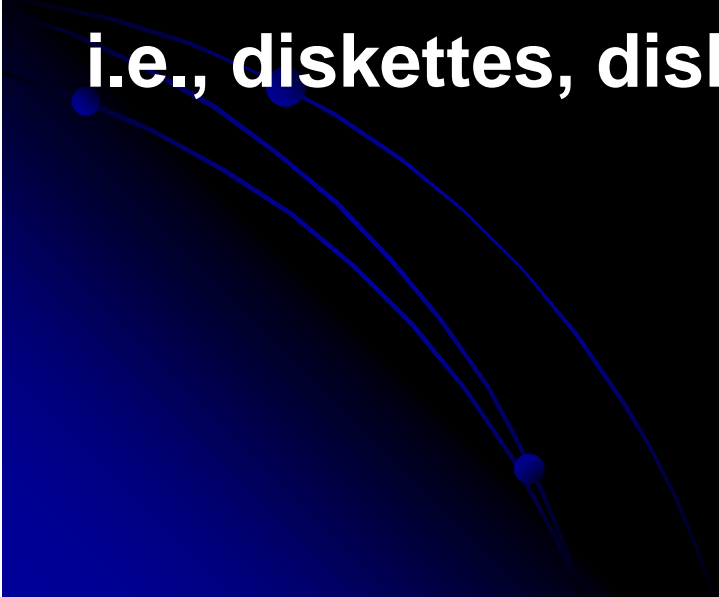
- **Customer medical information:**
 - ✓ stored in a separate secured location
 - ✓ noted in the customer's case file.
- **Confidential information stored electronically should have security programs in place to prevent unauthorized users from accessing this information.**

PROCEDURES—Storage of Confidential Information

Confidential information:

- should **not be left unattended** by authorized users
- **computer screens should be locked** before leaving the area (i.e. CTRL+ALT+DELETE)
- **authorized users should be conscious of information that is displayed on monitors** when interacting with unauthorized users

PROCEDURES—Storage of Confidential Information

- **Electronic media containing confidential information should be secured to prevent unauthorized access**
i.e., diskettes, disk drives, CD-ROMs, tapes, etc.
- 

PROCEDURES—Storage of Confidential Information

- **When staffing change occurs, it is the responsibility of the supervisor to ensure all confidential information is returned, and user access terminated as appropriate.**
- **The supervisor includes Access Request Form to DWD to inactivate system access.**

PROCEDURES—Sharing of Confidential Information

- Sharing confidential information is a necessity to operate the programs mentioned in Sections 2 & 3 of this plan.
- Any staff utilizing this information will need to complete the training, pass the test, and be a current member of the authorized user list.

PROCEDURES—Sharing of Confidential Information

- When transmitting paper copies of confidential information—place in folder or envelope marked, “**Confidential.**”
- When confidential information is **not being used**, it should be **placed in a secure location.**

PROCEDURES—Sharing of Confidential Information

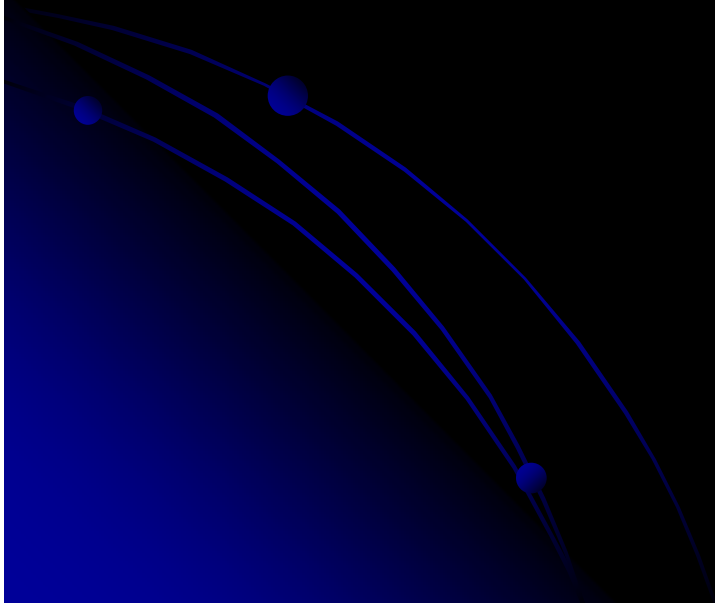
- **Confidential information** should be shared, when requested, in writing by law enforcement for investigative purposes.
- **Staff person** receiving the request must follow procedures outlined in the **DWD Media and Legislative policy**, which can be found on WorkSmart.

PROCEDURES—Destroying Confidential Information

- **Once paper copies of confidential information are no longer needed, documents should be disposed of according to applicable state and federal retention guidelines, using appropriate methods to maintain confidentiality**
(i.e., shredded on site, placed in a securely locked receptacle for shredding later)

PROCEDURES—Destroying Confidential Information

Per state policy, electronic documents and emails are archived and cannot be destroyed.



PROCEDURES—Breach of Confidentiality

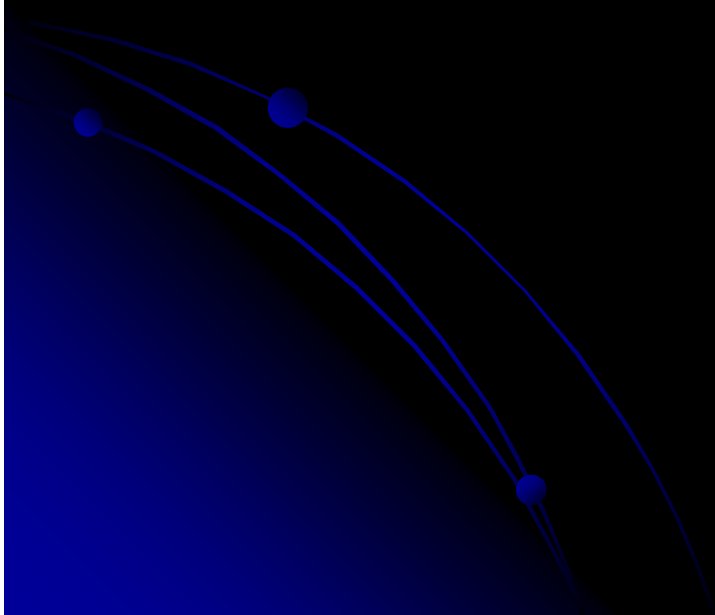
- **Any disclosure of confidential information (whether careless, accidental, or intentional) to unauthorized individuals is considered a breach.**
- **Unauthorized modification or deletion of information, or other violations of procedures are also considered breaches.**

PROCEDURES—Breach of Confidentiality (cont'd)

- **Information regarding a confidential information security breach is, on its own, confidential information and is not to be shared with anyone other than the immediate supervisor.**
- **Such actions may result in disciplinary, civil, or criminal action.**

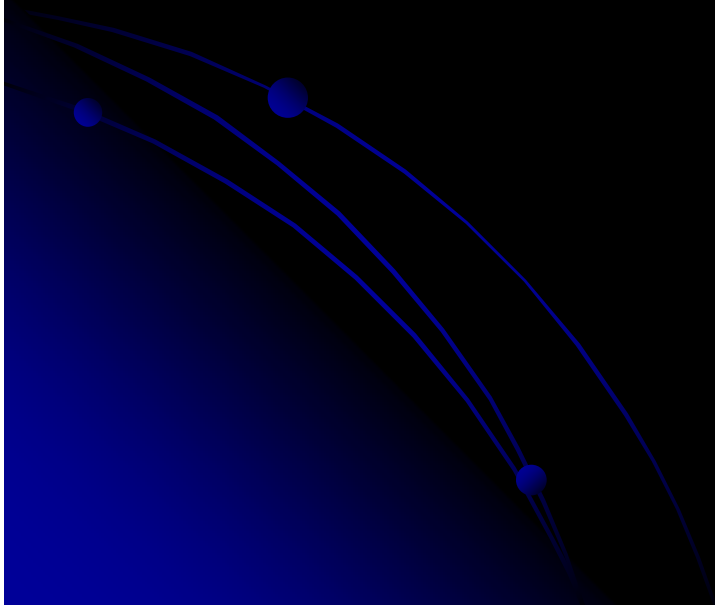
PROCEDURES—Breach of Confidentiality

- **If the breach involves information from DWD or partner agency, the user who discovered the breach must notify the supervisor immediately (not later than two business days)**

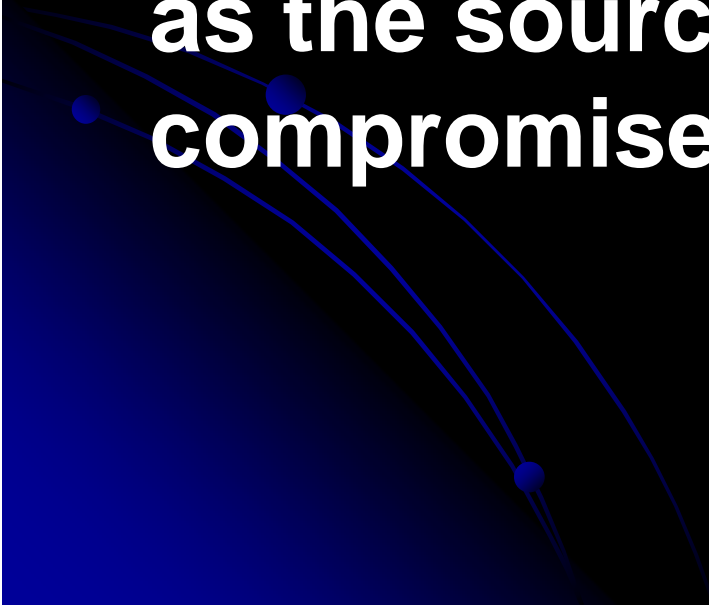


PROCEDURES—Breach of Confidentiality (cont'd)

- **It is the supervisor's responsibility to ensure notification is provided to the agency's appropriate up-line management.**




PROCEDURES—Breach of Confidentiality (cont'd)

- **If a breach occurs within DWD, the DWD Director (or assigned designee) will be responsible for notifying the partner agency acting as the source of information compromised.**
- 

PROCEDURES—Breach of Confidentiality **(cont'd)**

- **If the breach occurs within a partner agency, the Director from the partner agency is responsible to notify the partner agency that was the source of information compromised** (i.e. DWD or other agency listed in Section 1.4)

PROCEDURES—Breach of Confidentiality (cont'd)

- **If a breach occurs, the agency acting as the customer point of contact and source of information will be responsible for notifying the individual of the breach.**
- 

PROCEDURES—Breach of Confidentiality **(cont'd)**

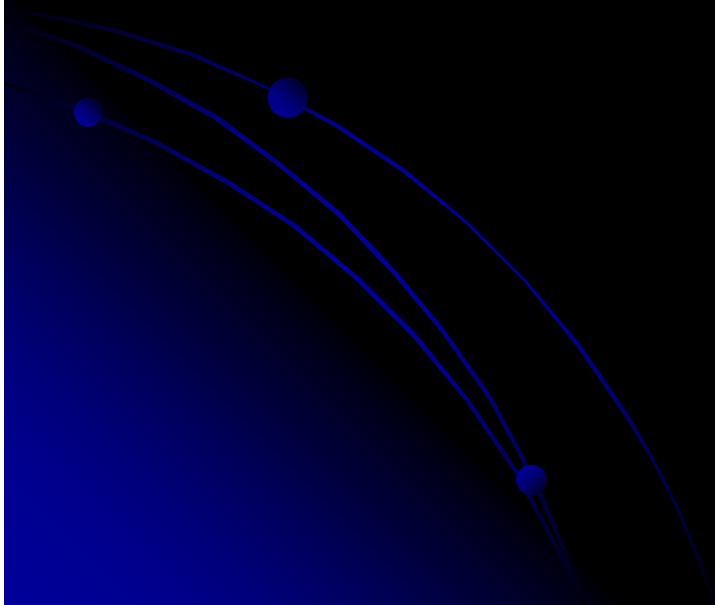
- **The U.S. Department of Labor's Training and Employment Notice #26-07, Job Bank Security Fraud Awareness, dated January 23, 2008, provides a list of resources for individuals and organizations to utilize regarding the prevention and reporting of cyber crimes.**

PROCEDURES—Breach of Confidentiality (cont'd)

- At <http://www.ic3.gov/>, individuals who suspect or know that they have been the victim of a cyber crime can file a report.
- This website is the **Internet Crime Complaint Center**, which is a partnership between the Federal Bureau of Investigation, the National White Collar Crime Center, and the Bureau of Justice Assistance.

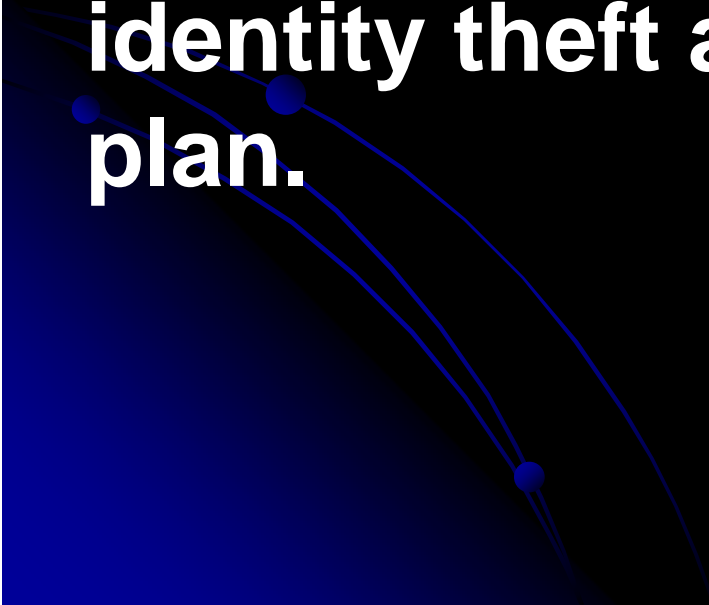
SOURCES

Following is a list of **state and federal legal provisions** that may affect the programs and services offered through the local workforce investment system.



SOURCES

This list should not be considered all inclusive. This listing is not exhaustive and a variety of other civil and criminal implications may surround confidential information or identity theft and may apply to this plan.



SOURCES

- State Code of Conduct Policy SP-13
- U.S. Department of Labor's Training and Employment Notice #26-07, *Job Bank Security Fraud Awareness*, dated January 23, 2008
- Revised Statutes of Missouri, Chapter 288, Section 250, Title XVIII, Labor and Industrial Relations
- Missouri's Safe at Home Act (2007)

SOURCES

- **Title III of the Social Security Act (SSA)**—
Statutory Confidentiality and disclosure requirements by this agency and use of Social Security number.
- The Federal Unemployment Tax Act (FUTA)
- **Public Health Service Act (PHSA)**
- The Health Insurance Portability and Accountability Act (HIPA)

SOURCES

- **The Family Educational Rights and Privacy Act (FERPA)**
- **The Family Medical Leave Act (FMLA)**
- **Freedom of Information Act (FOIA)**
- **The Open Records Act (Sunshine Act)**
- **The Age Discrimination in Employment Act**

SOURCES

- Title IV of the Civil Rights Act of 1964
- **Workforce Investment Act (WIA)**
- Any regulations and rules of Federal Personnel Law Governing Federal Employee's Behavior.

FORMS

Sample User Attestation Form

I understand that in the course of my employment with the (*Department/institution name*), I will receive or become aware of information that is sensitive or confidential. This information may be written, electronic, or verbal and come from a variety of sources. I understand that I am not to access sensitive or confidential information unless it is necessary in order for me to complete my job responsibilities. I further understand that (*Department/institution name*) policy on Confidentiality and Information Security applies to information I may inadvertently hear or see that does not directly involve me in an official capacity. I acknowledge that I must protect all sensitive or confidential information.

I understand that in the performance of my duties I may be requested to provide sensitive or confidential information to others. I agree to hold in confidence and to not disclose any sensitive or confidential information to any person, including employees of state, federal or local governments, except to those who have an official business reason for the information. Should I have questions regarding the proper handling and disclosure of confidential or sensitive information, I will immediately notify my supervisor for further clarification and direction prior to releasing the information.

If I willfully and knowingly disclose such information in any manner to any person or agency not entitled to receive information, I understand that I may be subject to adverse action, including corrective or disciplinary action, or possibly, personal liability.

I acknowledge that I have received the mandatory training, passed the quiz, and have read, understand, and will adhere to the _____ *Confidentiality*

Department / Institution name

and Information Security Plan and the above requirements.

Signature _____

Print Name _____

Date Signed _____

Original to official employee file (human resources) and copy to the Authorized User Registry

Toolbox Access Request Form

